Os Conflitos Cibernéticos como uma Ameaça Multidimensional[1]

Elói Martins Senhoras[2]
Fransllyn Sellynghton Silva do Nascimento[3]
Matheus Felipe Pereira de Souza[4]
Rita de Cássia de Oliveira Ferreira[5]
William Thiago Quirino Sales[6]
Yolanda Nunes Sousa[7]

Resumo

A guerra cibernética tem como referência as estruturas complexas de um novo padrão emergente de guerra, devido ao surgimento de novas tecnologias, *policymakers* (fazedores de políticas públicas) e comunidades epistêmicas. O presente artigo tem o objetivo de discutir as novas ameaças à segurança nas relações nacionais e internacionais que têm se espalhado no ciberespaço por meio de ações dos indivíduos, organizações e Estados. O artigo foi desenvolvido por meio dos procedimentos metodológicos de revisão bibliográfica em documentos, livros e periódicos científicos, bem como de estudos de casos, através de um mapeamento georeferenciado sobre os principais ciberconflitos em diferentes continentes (1990-2010), com o objetivo de subsidiar um estudo exploratório que se estruturou com base em uma lógica dedutiva de apreensão das questões complexas. Conclui-se que o conceito de segurança multidimensional é o mais adequado quadro teórico para explicar os conflitos cibernéticos, os quais inserem um novo tipo de espacialidade e a consequente pulverização do poder em uma ampla gama de agentes desde o Estado até os indivíduos, os quais não apenas se mobilizam por interesses distintos, mas também fazem uso de diferentes estratégias.

Palavras chave: Segurança Multidimensional, Guerra Cibernética, relações internacionais

---

[1]Esse artigo foi baseado no texto de SENHORAS e NASCIMENTO (2015) apresentado no *Congress of the Latin American Studies Association* – San Jose, Porto Rico, bem como no primeiro capítulo do trabalho de conclusão de curso em Relações Internacionais do NASCIMENTO (2015).

[2]Elói Martins Senhoras é professor titular do curso de Relações Internacionais da Universidade Federal de Roraima. É um dos líderes do Núcleo Amazônico de Pesquisas em Relações Internacionais – NAPRI, que desenvolve pesquisas nas áreas de Ciências Humanas e Ciências Políticas. E-mail para contato: eloisenhoras@gmail.com.

[3]FransllynSellynghton Silva do Nascimento é acadêmico do curso de Relações Internacionais da Universidade Federal de Roraima. Desenvolve pesquisas junto ao Núcleo Amazônico de Pesquisas em Relações Internacionais – NAPRI. E-mail para contato: lington@hotmail.com.

[4]Matheus Felipe Pereira de Souza é acadêmico do curso de Relações Internacionais da Universidade Federal de Roraima. E-mail para contato: mfpsl@hotmail.com.

[5]Rita de Cássia de Oliveira Ferreira é acadêmica do curso de Relações Internacionais da Universidade Federal de Roraima. Desenvolve pesquisas junto ao Núcleo Amazônico de Pesquisas em Relações Internacionais – NAPRI. E-mail para contato: rita_oferreira@hotmail.com.

[6]Willian Tihago Quirino Sales é acadêmico do curso de Relações Internacionais da Universidade Federal de Roraima. E-mail para contato: willian.tihago@gmail.

[7]Yolanda Nunes Sousa é acadêmica do curso de Relações Internacionais da Universidade Federal de Roraima. Desenvolve pesquisas junto ao Núcleo Amazônico de Pesquisas em Relações Internacionais – NAPRI. E-mail para contato: yoko_ns@hotmail.com.

Introdução

A interface reticular da *internet* possibilita a melhoria na comunicação entre os indivíduos, contudo também se tornou um instrumento de poder pelos atores estatais e não estatais, razão pela qual novas ameaças de natureza cibernética passaram a repercutir crescentemente nas relações nacionais e internacionais e no surgimento de plataformas militares e civis especializadas de segurança.

O surgimento de conflitos cibernéticos pode ser apreendido por distintas óticas tipológicas conforme o *modus operandi* dos atores nas ações litigantes, razão pela qual faz-se necessário delimitar, a despeito da multiplicidade de teorias, a existência de duas correntes, as quais são identificadas pelos enfoques minimalista e maximalista.

No enfoque *minimalista*, a ótica de visualização dos conflitos cibernéticos destaca a percepção estado centrica dos interesses nacionais nos conceitos cibernéticos, na qual os Estados Nacionais representam o núcleo concentrador de poder na difusão e atração conflitiva no espaço cibernético. Nesta perspectiva, destacam-se apenas dois conceitos, sendo eles: a ciberespionagem, como uso da Inteligência por meio do uso espaço cibernético e a ciberguerra ou guerra cibernética, como arte e estratégia dos Estados Nacionais para derrotarem um oponente sem derramar sangue por meio da invasão das redes de tecnologias de informação e comunicação de outros países (CLARK e KNAKE, 2010; CARR, 2011). Conforme Singer e Friedman (2014), os elementos-chaves da guerra no espaço virtual, ainda na perspectiva minimalista, possui semelhanças e conexões com outros domínios bélicos no espaço terrestre, marítimo e aeroespacial, representando, apenas uma nova espacialização interconectada às demais.

No enfoque *maximalista*, a concepção ampliada dos conflitos cibernéticos traz um alargamento analítico ao priorizar diversos atores descentralizados que atuam à margem do controle dos Estados Nacionais ou mesmo sob sua influência, impactando assim em diferentes padrões de interação litigante no meio cibernético, conforme o padrão distinto de ação e ideologia presente. A visão maximalista dos conflitos cibernéticos traz uma apreensão, tanto dos atores estatais quanto dos atores não estatais, na utilização de suas capacidades cibernéticas para atacarem, defenderem e espionarem, dentre outras finalidades políticas, econômicas e militares (HEALEY, 2014).

Segundo Dunn (2012), esta ótica maximalista dos ciberconflitos propicia uma maior compreensão da complexidade cibernética, ao vincular distintos atores com diferentes padrões de interação e centralização de poder, razão pela qual é possível visualizar uma escada cibernética com distintos degraus, desde o primário degrau do ciberativismo ou cibervandalismo, passando pelos segundo, terceiro e quarto degraus, com os crimes cibernéticos, a ciberespionagem e o ciberterrorismo, até se chegar ao último degrau, o conflito bélico no espaço virtual, a ciberguerra.

Tomando como referência estas discussões de vanguarda, a presente pesquisa de natureza exploratória quali-quantitativa foi desenvolvida com base tanto em uma revisão bibliográfica e documental, quanto em um georreferenciamento dos principais ciberconflitos no mundo.

O objetivo geral deste artigo é analisar as diferentes categorias de conflitos cibernéticos à luz de um recorte teórico metodológico weberiano de tipos ideais, findando revelar quais são os interesses dos principais atores envolvidos e a complexidade das agendas de segurança.

Por meio de uma lógica dedutiva, que parte de marcos históricos e teóricos a fim de subsidiar o estudo de caso da realidade, por meio de um georreferenciamento da ciberguerra no mundo, o presente artigo foi estruturado em quatro seções articuladas complementarmente entre

si, incluídas a presente introdução e as considerações finais.

Na primeira seção, “Paradigmas analíticos sobre os conflitos cibernéticos”, o artigo apresenta as principais macroconcepções ideológicas existentes nesta recente área de estudo, a fim de demonstrar os três grandes guarda-chuvas analíticos que convergem a pluralidade de teorias existentes.

Na segunda seção, “Marcos de periodização dos conflitos cibernéticos”, surge uma análise de conjuntura das principais dinâmicas de conflitos cibernéticos no globo, por meio da estruturação de um mapeamento georreferenciado das áreas que mais recebem ataques de natureza intra-estatal, de ativismo político ou de *crackers*.

Na terceira seção, “Planos de espacialização dos conflitos cibernéticos”, apresenta-se a complexidade espacial dos conflitos cibernéticos por meio da simultânea identificação de repercussão, tanto no mundo virtual quanto no mundo real, uma vez que existe um *continuum espacial*, no qual o espaço virtual transborda impactos sobre o espaço real.

Na quarta seção, “Atores dos conflitos cibernéticos”, a pesquisa introduz um sistema classificatório de atores portadores de interesses específicos e impactos nos diferentes conflitos cibernéticos, concebido por meio de quatro tipos ideais que projetam características específicas de capacidade técnica no ciberespaço, que podem ser fonte de ameaças para os países.

Por fim, as últimas considerações são tecidas à guisa de conclusão a fim de sintetizar as principais discussões abordadas na pesquisa, bem como apontar o dilema de segurança multidimensional engendrado pela ampla difusão de distintos padrões de conflitos cibernéticos nas relações inter e intra-nacionais.

Paradigmas analíticos sobre os conflitos cibernéticos

Nos estudos de segurança internacional, a apreensão empírica dos fatos tem tradicionalmente sido construída à luz de marcos conceituais e teóricos, razão pela qual na investigação dos conflitos cibernéticos faz-se necessário apreender os principais paradigmas analíticos sobre o assunto, os quais podem ser identificados pelas abordagens nacional-realista, liberal e híbrida.

A relevância do uso instrumental destes três paradigmas analíticos, se dá pela apreensão das principais linhas discursivas e ideológicas convergentes, sem recorrer a uma discussão exaustiva sobre uma pluralidade de teorias limitadas na explicação do complexo e mutável fenômeno dos ciberconflitos.

Em um primeiro plano, no *paradigma nacional-realista*, os ciberconflitos são entendidos como um fenômeno produzido pelos Estados nacionais no ciberespaço e com repercussão nos demais espaços materiais da guerra - terra, água, ar e aeroespacial - dentro de um jogo internacional de soma zero, no qual o rompimento de equilíbrio de poder representa o ganho de um Estado com base na perda de outro.

Nesse sentido, o espaço cibernético representa uma nova arena política de atuação dos Estados, na qual eles necessitam atuar a fim de projetar poder e influência para com outros Estados. A segurança cibernética fica em xeque a partir do momento em que tais Estados se capacitam e passam a ameaçar outros Estados com suas potencialidades cibernéticas.

Em um segundo plano, os ciberconflitos são apreendidos no *paradigma liberal* a partir de uma identificação reticular de conflitos promovidos pelo uso de Tecnologias de Informação e Comunicação (TICs), por uma pluralidade de atores com poderes centralizados e

descentralizados em um contexto de crescente interdependência complexa nas relações internacionais.

De indivíduos isolados a grupos de pessoas, passando pela participação de Estados nacionais ou mesmo organismos internacionais, os ciberconflitos se materializam pelas capacidades cibernéticas ofensivas, defensivas, de espionagem e Inteligência articuladas por diferentes *stakeholders* (HEALEY, 2013).

Em um terceiro plano, o ciberconflito pode ser analisado por enfoques ecléticos de conjugação de distintos marcos teórico-ideológicos sob a denominação de paradigma híbrido, a fim de mostrar como visões racionalistas de uma perspectiva liberal e nacional-realista podem funcionalmente dialogar com visões pós-modernas ou paradigmas críticos para mostrar a complexidade multidimensional das redes cibernéticas.

O enfoque de segurança multidimensional adquire importância à medida que explica porque a segurança cibernética, antes de ser exclusividade de uma ótica internacionalista, passa a ser visualizada dentro de uma agenda multidimensional, com repercussões em agendas securitárias tênues de natureza civil e militar que requerem classificações dos tipos de ciberconflitos e ciberatores (DAVID, 2001).

Com base nestes três paradigmas é possível observar as limitações teóricas frente aos fenômenos complexos e mutáveis, razão pela qual o artigo toma como referência de análise o enfoque de segurança multidimensional a partir da convicção de que o esforço analítico multidisciplinar, baseado na conjugação de forças, pode trazer novas reflexões sobre os ciberconflitos.

Recorrendo a um recorte analítico de tipos ideais e a uma revisão bibliográfica, o artigo abordará nas seções seguintes, respectivamente, os principais *atores (*crackers, hackers, hackers soldados e hacker ativistas) e *ciberconflitos* (cibervandalismo, cibercrimes, ciberespionagem, ciberterrorismo, ciberguerras), a fim de concluir com uma análise empírica conjuntural dos principais conflitos cibernéticos no mundo.

Marcos de periodização dos conflitos cibernéticos

A história de desenvolvimento dos conflitos cibernéticos está diretamente relacionada com a própria criação e evolução da Internet, ao longo de uma periodização que se inicia, embrionariamente, no pós II Guerra Mundial e se materializa como fenômeno global no século XXI.

Em um primeiro momento, a lógica conflitiva da Guerra Fria, entre as décadas de 1950 e 1980, foi a responsável pelo desenvolvimento militar de tecnologias de comunicação e informação, as quais embora, embrionariamente, tenham sido utilizadas para finalidades militares, viriam a impactar nas décadas seguintes no desenvolvimento civil da internet como meio de fluxo do espaço cibernético.

Em um segundo momento, com a difusão civil da internet em âmbito mundial, a partir da década de 1990, o espaço cibernético passou por uma crescente maturação conectiva, propiciando o surgimento espontâneo de ações oportunistas por diferentes atores centralizados ou descentralizados, que se caracterizaram como diferentes padrões de ciberconflitos conforme a agenda de motivação política, econômica, cultural ou militar.

Embora o espaço cibernético possua uma história recente de estruturação, seu impacto na humanidade é caracterizado como uma força profunda de longa duração, recriando dinâmicas

tradicionais e potencializando o surgimento de novas dinâmicas conjunturais que caminham por polarizações entre a integração e a fragmentação ou entre a convergência e o conflito.

Planos de espacialização dos conflitos cibernéticos

A espacialização dos conflitos cibernéticos pode ser compreendida pela manifestação das ações de diferentes *stakeholders* no ciberespaço, em função da nodulação das redes por meio de arranjos variáveis nos planos intra-nacionais e internacionais, o que significa dizer que todo ciberconflito tem uma simultânea espacialização, tanto no mundo virtual quanto no mundo real.

A multiplicidade de escalas espaciais existentes entre o mundo virtual e real, devido às redes infra-estruturais, softwares e protocolos de funcionamento, repercute em um dilema de segurança multidimensional caracterizado por ações coletivas de prevenção e proteção que repercutem sistemicamente na conformação de externalidades negativas de aumento dos conflitos.

A complexidade das novas ameaças cibernéticas traz consigo ações coletivas no ciberespaço que impactam em repercussões negativas conformando, tanto um *dilema multi-escalar,* em razão da compressão espacial entre o real e o virtual, ou ainda, entre o nacional e o internacional, quanto um *dilema multi-temática*, devido à complexa trama reticular, sincrônica e intercomunicável de ações estatais de Defesa, Segurança e Inteligência.

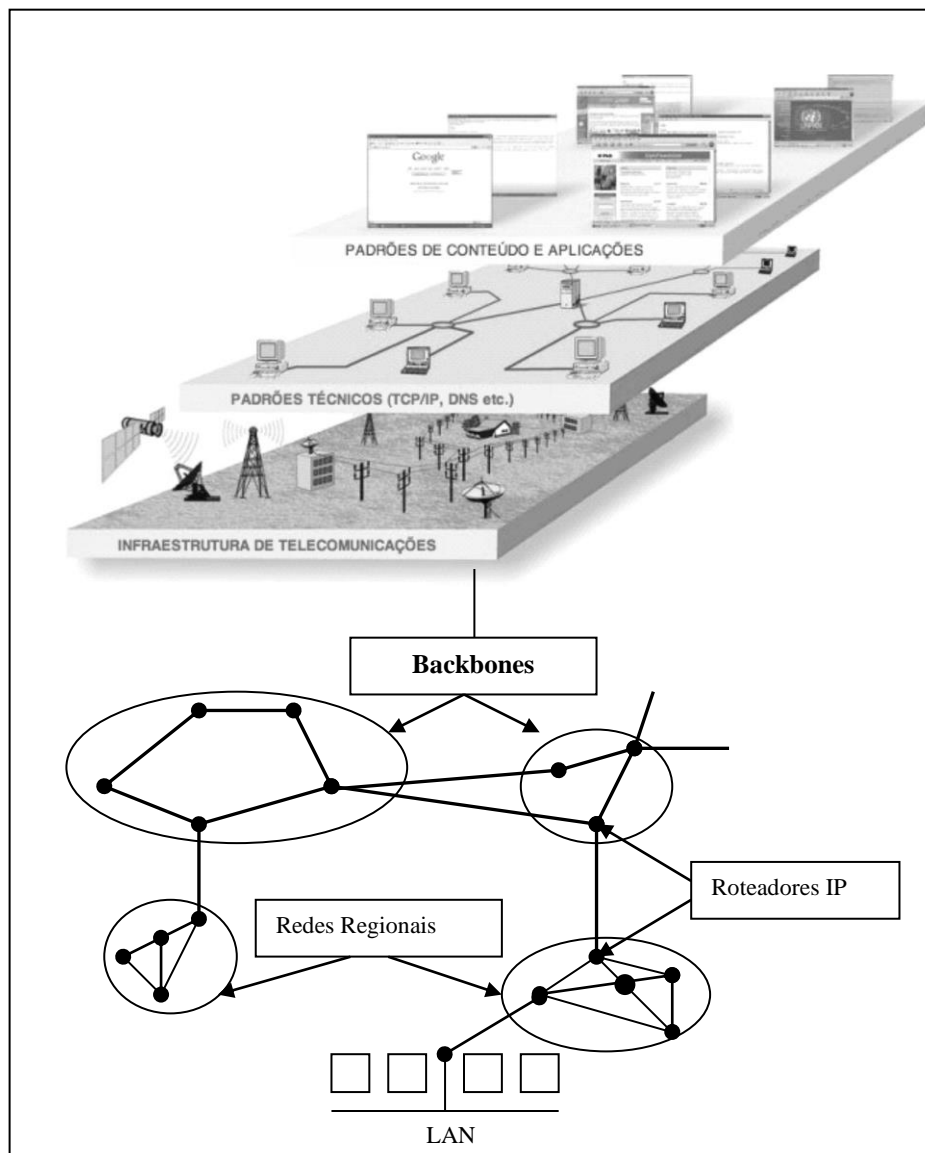
Entende-se por ciberespaço[8] o espaço de comunicação aberto pela interconexão mundial dos computadores e da memória dos computadores, nessa definição inclui o conjunto dos sistemas de comunicação eletrônica (os conjuntos de redes *hertzianas* e telefônicas clássicas), na medida em que transmitem informações provenientes de fontes destinadas a digitalização (LEVÍ, 1999).

Por um lado, o funcionamento do espaço cibernético é compreendido por três componentes básicos, os quais são classificados em infraestrutura física de telecomunicações, estrutura lógica com padrões técnicos, e, padrões de conteúdo e aplicações, sendo cada uma destas camadas propulsoras da internet e dos focos de manifestação dos diferentes padrões de conflitos cibernéticos.

Devido à sua criação e desenvolvimento multi-institucional descentralizado, o espaço cibernético se tornou ao longo do tempo em um complexo suscetível a conflitos, pois é permeado pela convergência de distintas tecnologias de informação e comunicação na rede conhecida como internet, caracterizando-se pela ausência de nodo central; pela flexibilidade arquitetural; pela redundância de conexões e funções e pela capacidade de reconfiguração dinâmica (SENHORAS, 2002).

---

[8]Essa palavra foi mencionada pela primeira vez na obra literária de ficção científica *Neuromancer* em 1984, de autoria de William Gibson, sobre um *hacker* em um mundo caótico e anárquico no futuro, este livro serviu de base para os filmes da trilogia *Matrix*.

Figura 1 - Complexidade do espaço cibernético

Fonte: **CPqD** (2001) *apud* SENHORAS (2002); KURBALIJA (2008) *apud* LUCERO (2011).

Por outro lado, o destino ou a origem de um ataque cibernético, por mais que se projete em um mundo virtual, assenta suas ações ou manifestações no mundo real por meio das redes infra-estruturais, funcionalmente utilizadas por redes variáveis intra-nacionais descentralizadas ou por arranjos internacionais de natureza unilateral, bilateral, plurilateral, regional ou mesmo multilateral.

De fato, o espaço virtual transborda impactos sobre tradicionais arenas espaciais de conflito, como a terra, mar, ar e espaço aéreo devido às conexões de interface com o mundo real, pois, mesmo representando-se como uma nova arena para a evolução progressiva dos conflitos, ele não apenas projeta antigos padrões de impacto material, mas também novos padrões de impacto virtual.

Um panorama exploratório no mundo mostra que as fronteiras nacionais e internacionais ou até mesmo limites entre o mundo real e virtual foram comprimidas pelo ciberespaço como um *locus* de uma quinta geração de guerra, quando diferentes *stakeholders* conduzem conflitos desenvolvidos por indivíduos, pequenos grupos, organizações, grandes redes ou até mesmo países, ou quando as políticas de Segurança, Defesa e inteligência entrecruzam suas funções contra as novas ameaças, embora com eficiência questionável e legitimidade.

Atores dos conflitos cibernéticos

No espaço abstrato da rede internacional de computadores, a internet é um componente, fundamentalmente, de operação humana que ao longo do tempo cristalizou um padrão de interação diária, cuja repercussão foi consolidar um macro espaço, conhecido como ciberespaço ou espaço virtual, cujas atividades complementam e podem transbordar impactos positivos ou negativos nos espaços reais (terra, água, ar e sideral).

Cristalizado pela difusão da internet, o ciberespaço é o palco de uma série de *stakeholders*, atores portadores de interesses específicos nas atividades de impactos dos conflitos cibernéticos, os quais podem ser identificados por cinco categorias - *hackers*, *hackerssoldados*, *hacker ativistas*, *crackers e hackers terroristas*– em razão da capacidade técnica no ciberespaço.

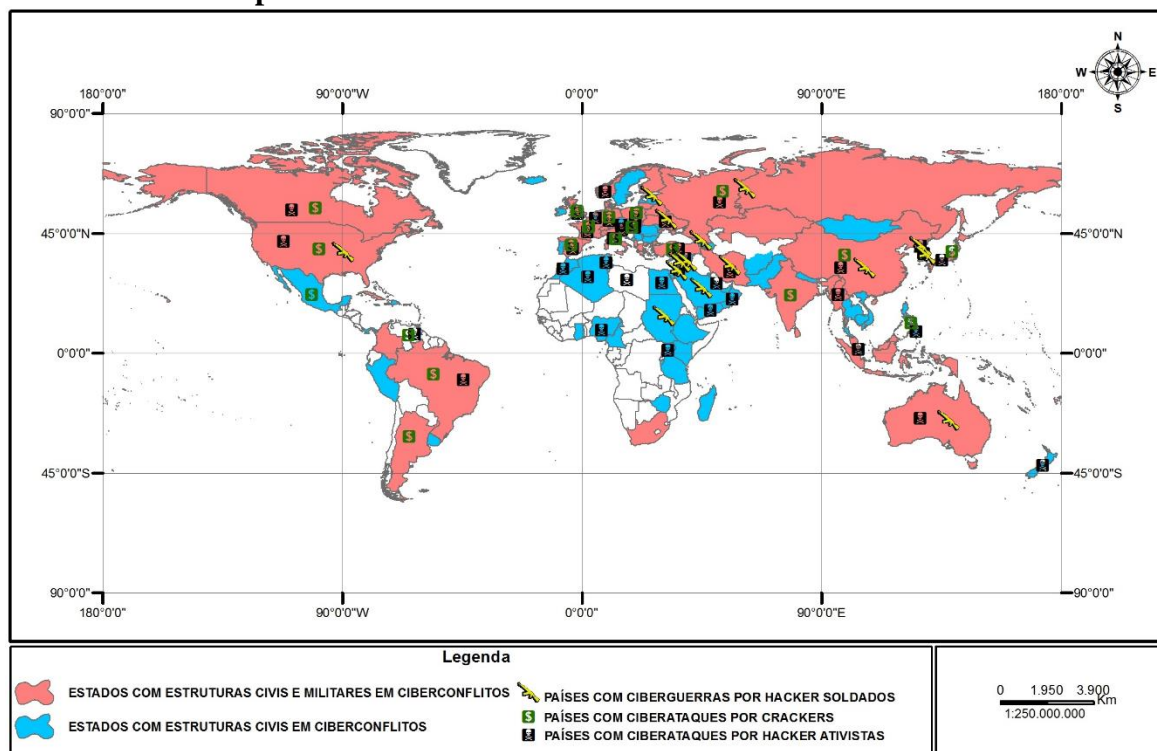
Quadro 1 - Tipologia weberiana de atores promotores de ciberconflitos

Tipos de hackers	Tipo de Conflito	Instituição repressora	Ideologia
Hackers	Crimes de privacidade e direitos autorais	Estados	Liberdade da rede
Hackers soldados	Ciber guerras	Estados	Nacionalistas
Hackers ativistas	Ciber vandalismo	Estados	Depende do grupo
Crackers	Crimes econômicos da internet	Estados, Empresas e Organizações Internacionais	Ganhos financeiros
Hacker terrorista	Ciber terrorismo	Estados e Organizações Internacionais	Depende do grupo

Fonte: Elaboração própria. Baseada em Castell (2003); Cavelty (2010); Healey (2014).

Os referidos *stakeholder s*abordados possuem uma clara adesão analítica em relação aos cinco tipos de conflitos no ciberespaço, que acendem numa escada crescente: o primeiro, *cibervandalismo* praticado pelos *hackers* ativistas; o segundo, *crimes da internet* realizados pelos *crackers*; o terceiro, *ciberespionagem* desenvolvido pelos *hackers* soldados e *crackers*; o quarto, *ciberterrorismo* executado pelos hackers terroristas e o quinto, *ciberguerras* onde os atores são estatais, como os *hackers* soldados, ou não estatais, como os *hackers* ativistas e terroristas (CAVELTY, 2010).

A espacialização dos campos de poder[9] existentes nos conflitos foi desenvolvida com base em um mapeamento georeferenciado, que sistematizou a compilação de recortes de jornais nacionais e internacionais, bem como de documentos e relatórios de organizações internacionais, como o “Cyber Índex” da Organização das Nações Unidas, e de empresas, como o “*Internet securitythreatreport*” da Symantec Corporation.

Mapa 1 - Estruturas estatais de ciberconflitos no mundo

Fonte: Elaboração própria. Relatório de dados compilados em Senhoras (2014).

Conforme no mapa acima é possível observar que a maior parte dos conflitos estão localizados no Hemisfério Norte, em países que dispõem de ótima conexão à internet. Nesse cenário, no Brasil ocorrem ciberataques de crackers e hackers ativistas, mas por ser uma nação em tempos de paz não ocorrem ciber guerras. Mesmo assim é necessário entender quem são os atores bem como suas interações, que justificam os conflitos cibernéticos serem uma ameaça multidimensional.

Em primeiro lugar, engendrando conflitos ligados aos direitos autorais e de privacidade no espaço virtual, encontram-se os *hackers*, os quais são indivíduos com habilidades de entrar em sistemas de computadores, caracterizados como profissionais e estudantes que participam do

---

[9] Campo de poder é uma arena onde ocorre diferentes estratégias de conflitos e cooperação entre os atores, nesse cenário o poder é relacional entre forças de atração e repulsão denominados de polos de poder, como os polos magnéticos, sendo toda relação um lugar de poder, isso significa que os polos estão ligados a manipulação dos fluxos que atravessam e desligam as relações, os quais são energia e a informação, essa combinação de variáveis podem serem analisados como vetores, a saber um poder informacional, poder energético e poder mediano (RAFFESTIN, 1980).

movimento de *software* livre, contribuindo para a inovação na internet, pois fazem uma ligação entre o conhecimento do meio científico para o empresarial (CASTELL, 2003).

Os fenômenos conflitivos que *hackers* engendram são identificados como crimes por direitos autorais por defenderem a liberdade de conteúdo na internet e a defesa da privacidade dos usuários, diante das ações dos atores estatais. Esse seu relacionamento com o Estado é de um campo de cooperação relativo por que ora incentivam a ações empreendedoras dos hackers, ora punem contrapor suas ações.

Em segundo lugar, os *hackers soldados* são atores responsáveis por defender os seus países de ataques virtuais por meios de plataformas de defesa, que podem atuar de caráter ofensiva, atacando pretensos inimigos, como nos EUA, ou defensivo, como exemplo o Brasil, onde esses soldados virtuais são bem qualificados, sendo possível a admissão de civis com notável saber de sistemas de computadores, desde que estejam de acordo com a doutrina das Forças Armadas.

Os referidos guerreiros virtuais agem nas ciberguerras e fazem parte do aparato de defesa de um Estado-Nação, com a principal função de defender as infraestruturas críticas, no qual o seu desligamento ou interrupção traria grandes danos para a sociedade. A relação entre *hackers* soldados é ora de cooperação e ora de conflito e vai depender do contexto político, pois admite a possibilidade de exercícios conjuntos e tratados de cooperação entre os países. Mesmo assim, de modo estrutural, todas as nações executam algum ataque cibernético secreto, até mesmo entre aliados. Já no quesito interação com os *hackers* ativistas é de repulsão, por entender ser uma fonte de ameaça.

Em terceiro lugar, vêm os *hackers ativistas*, definido por Healey (2014), como aqueles que conduzem suas atividades no interesse de uma ideologia. Deste modo, abre-se um amplo leque de interesses, desde um ato de ciber vandalismo de caráter conjuntural, que pode influenciar somente o espaço virtual, até a ação de grupos de *hackers* ativistas mais organizados como os *Anonymous* e os *Cypherpuks*, os quais podem promover manifestações no plano virtual e real.

Os *hackers ativistas*praticam o ciberativismo. Para Di Felice (2013), esse termo surge nos anos 1990 como um tipo de participação baseada na construção de redes informativas, pela difusão de informações e transformações da capacidade interativa da *Web*[10], que nos últimos anos tem sido uma forma intensiva de interação em rede entre indivíduos, territórios e tecnologias digitais, designativa da conectividade característica da ação social *em* e *nas* redes. Nos campos de poder, os *hackers* ativistas engendram repulsão com os *hackers* soldados e o Estado, e a cooperação com outros ativistas com ideologias convergentes.

Em quarto lugar, os atores identificados como *crackers* - do inglês *crack*, que significa quebrar – são especializados em cibercrimes de quebra de códigos para roubar senhas para finalidade criminosa. A atuação deste grupo de atores está relacionada com o aumento do comércio eletrônico no mundo, motivo pelo qual, no âmbito do combate a esses crimes, surgiu cooperação entre países por meio das organizações internacionais.

Os *crackers* executam crimes econômicos na Internet, que a Interpol (2015) sistematiza em três tipos: primeiro, os crimes financeiros e de corrupção; segundo, abuso como exploração

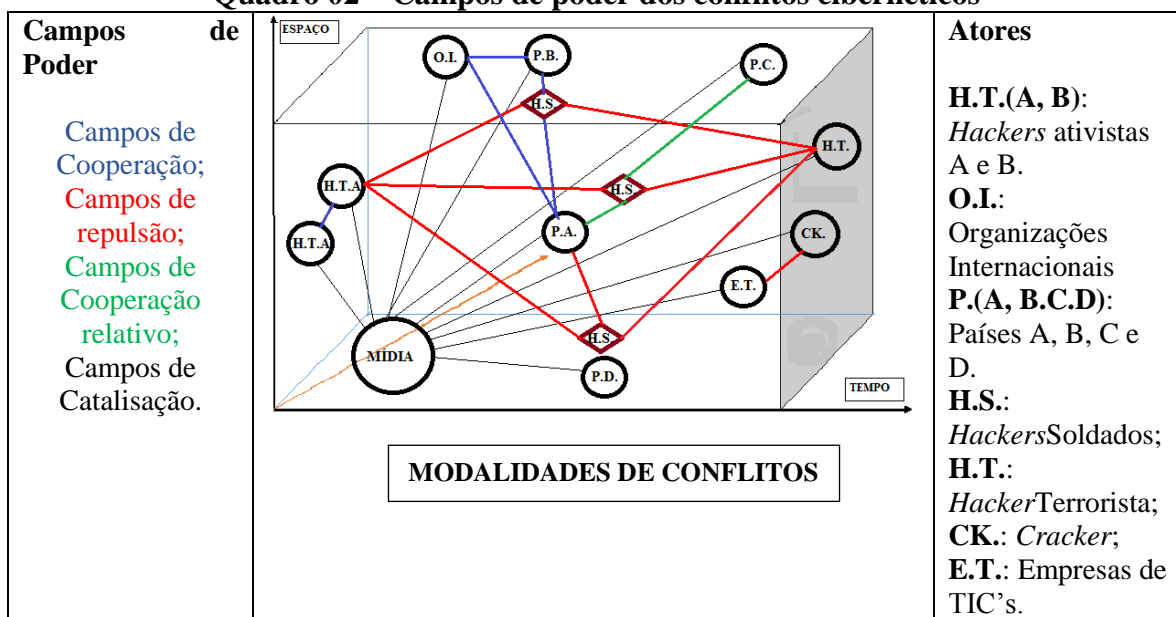
[10] Refere-se ao avanço nos conjuntos de técnicas para *design* e execução de páginas da web (sítios eletrônicos): *Web* 1.0 é estático sem interatividade com os leitores, a *Web* 2.0 as páginas possuem maior interação com o público e a Web 3.0 os conteúdos das páginas são personalizados para cada usuário (FAPCOM, 2014).

sexual e pedofilia e terceiro, ataques contra *hardware* e *software*, práticas que eram cometidas por indivíduos e grupos pequenos no passado. No século XXI, existem organizações criminosas que trabalham com *crackers* para cometer crimes, podendo até financiar atividades ilegais. Nos campos de poder possuem repulsão para com as empresas, países e organizações internacionais.

Em quinto e último lugar, a expressão *hacker terrorista* refere-se a um grupo de indivíduos ligados a uma célula terrorista, com capacidade técnica para fazer um ataque cibernético a um Estado. A definição é subjetiva à medida que o conceito depende de como cada Estado encara o terrorismo, sendo alguns *hackers ativistas* tipificados como grupo terrorista, como exemplo os Estados Unidos que assim consideram, já que qualquer divulgação de dados sigilosos é entendida como ação terrorista.

Esses atores, conforme Chen (2014), praticam operações com motivações políticas com intuito de causar graves prejuízos, como a perda de vida e danos econômicos graves, para tanto tem-se três partes: primeiro conduzido politicamente; segundo com efeitos graves e terceiro redes de computadores como meio. No quesito campos de poder, os *hackers* terroristas possuem campos de repulsão com hackers soldados e países.

Quadro 02 – Campos de poder dos conflitos cibernéticos

Campos de Poder		**Atores**
Campos de Cooperação; Campos de repulsão; Campos de Cooperação relativo; Campos de Catalisação.		**H.T.(A, B)**: *Hackers* ativistas A e B. **O.I.**: Organizações Internacionais **P.(A, B.C.D)**: Países A, B, C e D. **H.S.**: *Hackers*Soldados; **H.T.**: *Hacker*Terrorista; **CK.**: *Cracker*; **E.T.**: Empresas de TIC's.

Fonte: Elaboração própria. Baseada em: RAFFESTIN (1980).

No quadro acima, baseado em Raffestin (1980) sintetiza o que foi mencionado e faz uma projeção, quanto maior o espaço cibernético (variável espacial) e a duração do tempo (variável quantitativa), maior será a quantidade dos conflitos cibernéticos engendrados. Nesta análise existe, a manifestação de campos de poder com forças vetoriais, ora convergente ora divergente, por meio de uma geopolítica de conflitos cibernéticos que surgem com uma agenda de planos intra-nacionais e internacionais.

Por fim, independente dos interesses projetados pelos *stakeholders* no espaço cibernético, este proporciona tanto um melhor meio de comunicação entre os povos quanto um instrumento de projeção de poder para prejudicar outros atores, seja por razões financeiras, ideológicas ou políticas, demonstrando um problema de insegurança multidimensional, contrarrestada por instituições, nem sempre com intercoordenação institucional.

Conclusão

O desenvolvimento do ciberespaço propiciou a conformação de dinâmicas de convergências e conflitos em um complexo caracterizado por polarizações e paradoxos entre diferentes *stakeholders*, repercutindo em um dilema de segurança multidimensional que se caracteriza por contradições da ação coletiva não coordenada e pelo conseguinte surgimento de externalidades negativas.

O dilema de segurança multidimensional traz consigo uma percepção de aumento dos riscos securitários, tanto em função da reticularidade e influência recíproca entre as diferentes escalas espaciais do mundo real e virtual, quanto em razão da conformação de uma trama pouco transparente entre as ações sincrônicas de Defesa, Segurança e Inteligência.

Neste contexto, a soberania do Estado moderno, consubstanciada por construções internas dos direitos civis, encontra-se em uma contraditória crise devido à grande lacuna que se instala entre o discurso político e as políticas de securitização pelos Serviços de Inteligência e Espionagem, que passam a concentrar crescente força em relação aos interesses individuais a fim de preservar a ordem e promover o interesse nacional contra ameaças assimétricas.

Alguns conceitos polarizados, como segurança nacional e internacional ou interesse individual e nacional têm mudado de posição ou até mesmo passado por processos de hibridação perigosos para as políticas públicas, em um contexto de crescente promoção da segurança cibernética por meio de um Estado Big Brother, independentemente da natureza diferenciada das intenções criminosas geradas por *crackers*, a fim de se obterem ganhos econômicos em comparação a ampla gama de intenções políticas e ideológicas de *hackers*.

Por um lado, sob o prisma maximalista, uma multiplicidade de *stakeholders* intervenientes no ciberespaço demonstra que as novas Tecnologias de Informação e Comunicação (TICs) têm impactado na diminuição da soberania operacionais dos Estados, em razão de ações oportunistas de *crackers* (atores com intenção criminal) e *hackers* (ciberatores ativistas, terroristas e soldados) que tornam a *internet* um complexo problema.

Poucas ações de danos, utilizadas no ciberespaço, realmente representam declarações de guerra contra países, embora a maioria delas constituam atos criminosos, ideológicos ou políticos por redes de atores descentralizados com elevados impactos negativos sobre a sociedade civil, razão pela qual se identifica uma difundida tendência de securitização do espaço cibernético, sob a influência de determinados atos de discurso de natureza política e auto-referenciada.

Por outro lado, sob o prisma minimalista, a ativa participação de alguns países no mundo não-cinético através da espionagem, sabotagem e intervenções preventivas de ciberataque ou ciberdefesa, reintroduziu um problema para o uso da força pelos Estados devido ao retorno a um estágio *jus ad bellum* focalizado nos direitos do Estado para fazer guerras ou propriamente ciberguerras.

Os interesses intra-nacionais e internacionais afetados pelo mundo cinético das ciberguerras dividiram não só o consenso multilateral do princípio *jus in bellum*, promovido pela Organização das Nações Unidas (ONU) para restringir o uso da força, mas também gerou um novo padrão de conflito com perigosos contornos em relação aos direitos individuais, devido ao uso das mais modernas agendas de securitização.

Com base nestas discussões, subsídios foram fornecidos para uma melhor compreensão dos complexos impactos da cibernética e da informática na sociedade, ao projetarem a pulverização do poder em uma ampla gama de atores, desde o Estado até os indivíduos, os quais

são movidos não só por uma série de interesses diferenciados, mas também por distintas estratégias.

Referências bibliográficas

CASTELL, M. **A galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar 2003.

CLARKE, R. A; KNAKE, R. K. **Cyber War**: **the next threat to national security and what to do about it**. New York: HarperCollins, 2010.

CAVELTY, M. D. "Cyberwar: concept, status quo, and limitations". **CSS Analysis in Security Policy**, n. 71, April, 2010.

CHEN, T. M..**Cyberterrorism after Stuxnet.**Strategic Studies Institute and U.S. Army War College Press. Pennsylvania: U.S. Army War College Press, 2014. 44 p..Disponívelem: < www.carlisle.army.mil>. Acesso em: 16 de maio de 2014.

DAVID, C. P. **Segurança Cooperativa e Segurança Comum**. Lisboa: Instituto Piaget, 2001.

DI FELICE, M. Ser redes: o formismo digital dos movimentos net-ativistas. Revista Matizes – USP. v.7 n. 2, p. 49-71. 2013. Disponível em: <www.matrizes.usp.br>. Acesso em: 13 de fevereiro de 2015.

HEALEY, J. **A Fierce Domain: Conflitct in Cyberspace 1986 to 2012**. Arlington, VA: CCSA, 2013.

INTERPOL. Cybercrime. 2015. Disponível em: < http://www.interpol.int>. Acesso em: 12 de abril de 2015.

LÉVI, Pierre. **Cibercultura.** Ed. 34, 1999. p. 94-95.

LUCERO, E. **Governança da internet: Aspectos da formação de um regime global e oportunidades de ação diplomática**. Brasília: FUNAG, 2011.

NASCIMENTO, F. S. S..**MULTIDIMENSIONALIDADE DOS CONFLITOS CIBERNÉTICOS**. Trabalho de Conclusão de Curso (Graduação) – Universidade Federal de Roraima, Boa Vista, 2015.

PAGANINI , P.. "What is the Deep Web? A first trip into the abyss". Security Affairs, Maio de 2012. Disponível em: <www.securityaffairs.co>. Acesso em: 06 /06/ 2013.

RAFFESTIN, C.. **Por uma Geografia do Poder**. São Paulo: Editora Ática, 1980.

SENHORAS, E. M. "Discutindo o e-Governo e a Questão da Infoinclusão". **Anais do IX Simpósio de Engenharia de Produção**. Bauru: UNESP, 2002.

SENHORAS, E. M. **Mapas de ciberconflitos no mundo: relatório de pesquisa organizado para Congresso Acadêmico de Defesa Nacional**. Boa Vista: UFRR, 2014.

SENHORAS, E. M. "A diplomacia brasileira à luz de marcos estruturais e conjunturais de crise". **Boletim Mundorama**, vol. 92, Abril, 2015. Disponível em: <www.mundorama.net>. Acesso em 01/04/2015.

SENHORAS, E. M.; NASCIMENTO, F. S. S.. O Dilema da segurança multidimensional no paradigma cibernético. In: Congresso f the Latin American Studies Association. **Anais...**. Porto Rico: LASA, 2015.

SYMANTEC. **Internet security threat report 2014**. Mountain View: Symantec, 2014. Disponível em: <www.symantec.com>. Acesso em 01/04/2015.

UNIDIR - United Nations Institute for Disarmament Research. **The Cyber Índex: International Security Trends and Realities**. Geneva: UN, 2013.